Patent
Attorney's Docket No. 030681-291

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
A-jung Kim	Group Art Unit: 2135
Application No.: 09/816,080	Examiner: BEEMNET W. DADA
Filed: March 26, 2001	Confirmation No.: 7143
For: KEY AGREEMENT METHOD IN SECURE COMMUNICATION SYSTEM USING MULTIPLE ACCESS METHOD	

REQUEST FOR RECONSIDERATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In reply to the final Office Action dated March 1, 2005, applicants respectfully request reconsideration of the above-captioned application. Claims 1-6 are currently pending.

The Office Action includes a rejection of claims 1-6 under 35 U.S.C. §103 as allegedly being unpatentable over the Lo et al patent (U.S. Patent No. 5,732,139) in view of the Mazourenko et al patent (U.S. Patent No. 6,272,224). This rejection continues to be traversed.

The Lo et al patent discloses in columns 5 and 6 a scheme for quantum key distribution referred to as "BB84" after Bennett and Brassard in 1984. Basically, it involves a first user, Alice, which generates and sends a second user, Bob, a sequence of photons whose polarization she has chosen at random and does not inform anyone, including Bob, of the polarizations. Bob measures the polarizations using either rectilinear or diagonal basis with equal probability and records his chosen *basis* and his measurement results. Bob announces over a public channel,

for each photon, which basis he has chosen, but not the measurement result. Alice informs Bob publicly for each photon whether he has made the measurement along the correct basis. Alice and Bob then discard all cases in which Bob has made the measurements along the wrong basis and keeps only the ones that Bob has made along the correct basis.

Similarly, the Mazourenko et al system involves Alice generating and sending Bob a sequence of photons, each photon representing an information bit. Alice chooses two phase shifts at random separated by $\pi/2$ for the modulation signal to encode the 0 and 1 bits. Bob then attempts to determine which bit was sent by Alice by varying the phase shift of his modulation signal at random, using the two values. Bob then publicly informs Alice when he detects a photon but does not reveal the phase that he uses. It appears that Bob does not detect a photon when he does not happen to use the appropriate phase shift. Bob and Alice then eliminate all bits for which Bob did not detect anything. The remaining bits are used to form a common encryption key. See column 8, lines 50-67, for instance.

The modification suggested in the Office Action appears to eliminate one communication string from Alice to Bob and there appears to be a difference insofar as Bob apparently cannot measure photons from Alice unless he happens to choose the correct phase shift, for reasons that are not completely understood. What is clear, however, from the disclosures of the Lo et al and Mazourenko et al patents is that neither adopts only bits having a measured value beyond a threshold value, which is predetermined, in contrast to the recitations of present claim 1 for instance. Instead, the Lo et al patent transmits from Bob to Alice the measurement *basis*. In the Mazourenko et al system, Bob informs Alice of *when* photons are detected.

Neither employs a threshold basis for separating the bits to those that are adopted and those that are not. This threshold mechanism of the recited invention potentially has a number of significant advantages as explained in paragraphs 0047 through 0051 of the present application. For instance, a basic principle of making no correlation between the measurement results of the users and those of the eavesdropper is not limited to optical communications but can also be employed by conventional wired and wireless communications. Hence, the range of the application of embodiments of the present invention is relatively unlimited. Also, the present invention in various embodiments exploits noises induced in the system, which means that the equipment does not necessarily have to be of high quality and high resolution. Additionally, embodiments of the present invention could be retrofit into conventional communication systems without substantial equipment improvements. The user can also use the same physical channel to deliver encryption keys and data text. There are many other potential advantages of the present invention, which are neither present nor suggested by the applied art. While advantages of an invention are not generally claimed, they nevertheless require consideration by the Office insofar as the question of obviousness invention is to be determined taking into consideration the invention as a whole. The fact of the matter is that neither of the applied prior art uses a threshold value as a determination as to which bits are adopted and which bits are not. Instead, the phase and phase shifts are employed, which limits the use of the applied art to various optical systems and cannot achieve the potential advantages of the present invention, which include the additional advantage of being able to change a degree of security.

In light of the foregoing, applicants respectfully request reconsideration and allowance of the above-captioned application. Should any residual issues exist, the Examiner is invited to contact the undersigned at the number listed below.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: July 1, 2005

By: _____
Charles F. Wieland III
Registration No. 33,096

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

VA 744575.1